Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF Ignite – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 28/08/2024 |
| **Link** | tryhackme.com/r/room/ignite |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 28/08/2024 | Produção |
| **1** | 02/09/2024 | Revisão |
| **2** | 02/09/2024 | Aprovação |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[User.txt 3](#_heading=h.3znysh7)

[Root.txt 3](#_heading=h.2et92p0)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

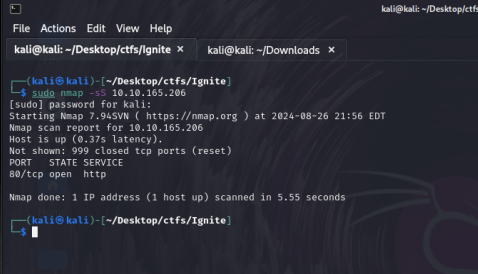
Ignite" do TryHackMe é um desafio de nível fácil que envolve um serviço CMS vulnerável e a obtenção de um shell reverso para escalar de um acesso inicial até privilégios de root,

**Desenvolvimento**

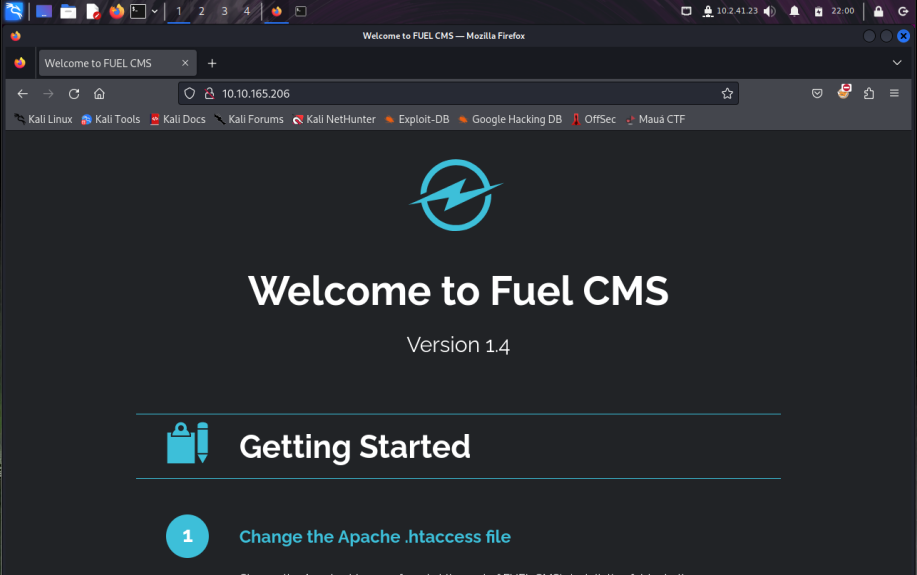
**User.txt?**

Começamos utilizando o nmap para poder descobrir as portas que estão abertas no servidor, porém apenas uma só está, a porta 80

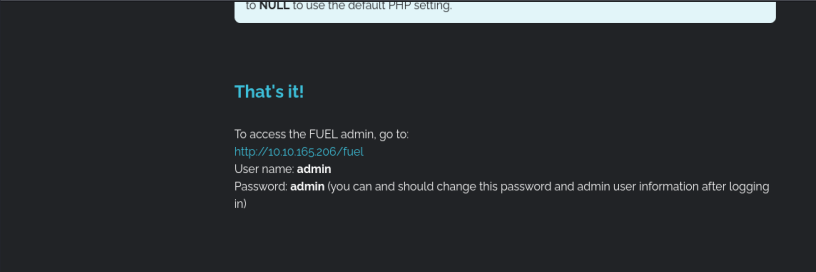
Comando usado: ***nmap –sS <ip\_machine>***

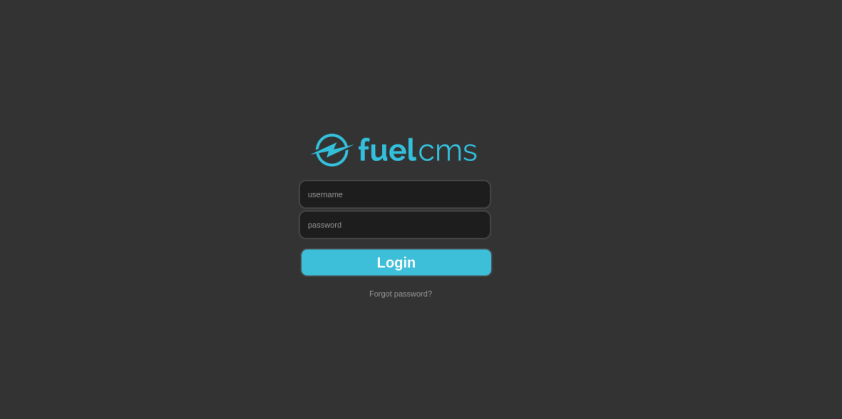


Acessando o site, já podemos analisar a página web e o seu versionamento, que é a 1.4. Podemos então depois pesquisar para ver se tem algum exploit.

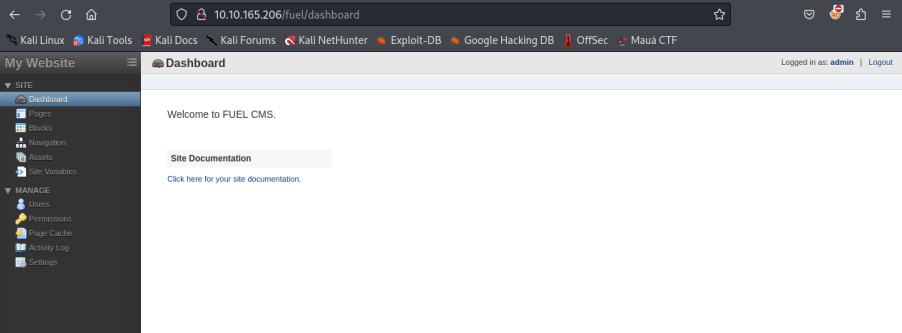


Descendo mais um pouco, poemos ver que ele está nos passando a página do admin e suas credenciais.



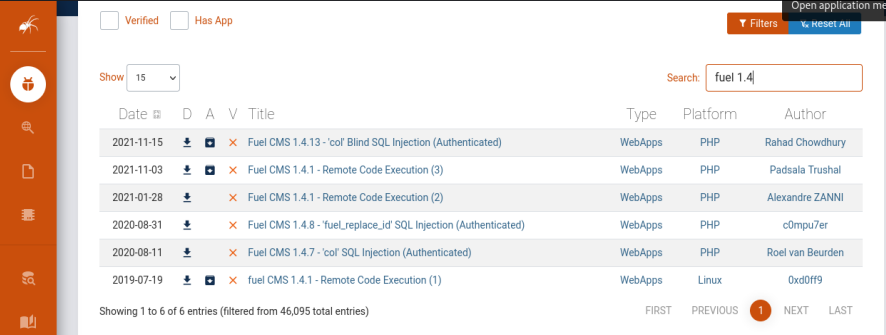


Acessando e dando uma olhada pela página, podemos ver que não há nada a ser feito aqui, portanto, não é este o caminho.



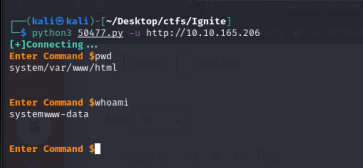
Pesquisando no <https://www.exploit-db.com/> podemos analisar que há diversos exploit’s para o “fuel 1.4”, vamos baixar algum e vê se conseguimos acesso.

Eu baixei o “2021.11.03”



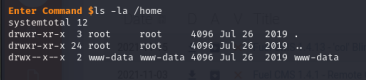
Após baixar e rodar o comando com o <ip\_machine> podemos então ter um acesso, só que muito restrito, podendo só rodar comandos muito simples.

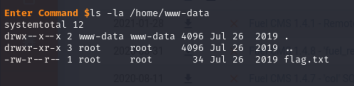
Comando usado: ***python3 (arquivo\_exploitdb) –u http://<ip\_machine>***



A gente pode navegar através de arquivos para poder acessar a primeira flag.

Comando usado: ***ls –la /###***



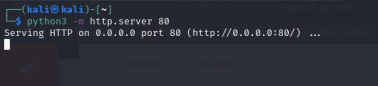


**Root.txt?**

Já que temos um certo acesso ao servidor, podemos então baixar uma reverse shell para podermos ter o acesso completo e melhorado.

Criando então um server local com o python, podemos baixar o reverse shell no servidor do <ip\_machine>

Comando usado: ***python3 –m http.server 80***

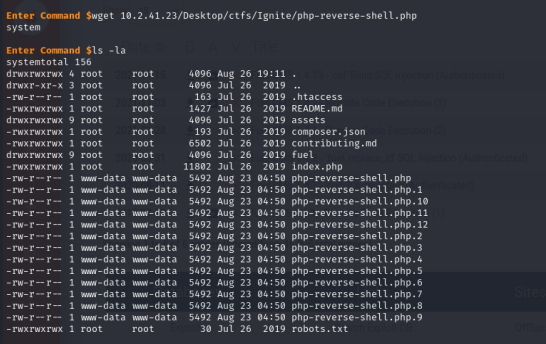


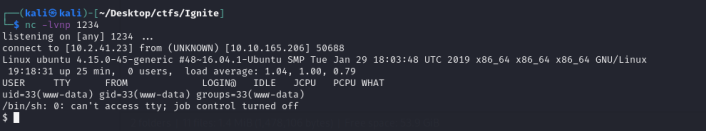
Abrindo um netcat na porta 1234, para poder já acessar quando rodarmos o arquivo da reverse shell

Comando usado***: nc –lvnp PORT***

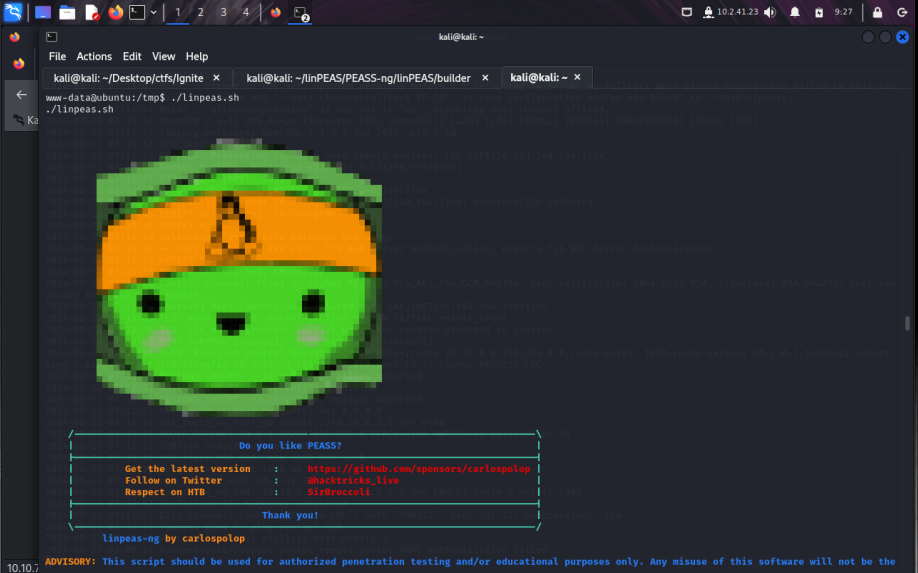


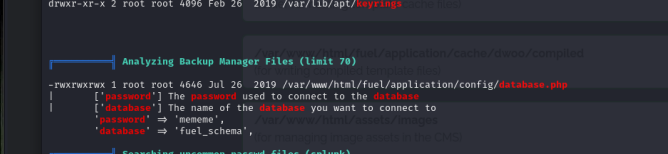
Baixando o reverse shell e executando através da url, podemos ter acesso





Usando o linpeas, ele descobre para a gente a senha do root e então podemos ter acesso sudo.







**Conclusão**

O ignite é um CTF simples, porém envolve criatividade e atenção, para poder realiza-lo.

**Referências**

[**https://www.exploit-db.com/**](https://www.exploit-db.com/)